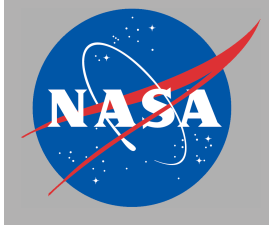
NATIONAL AERONAUTICS
AND SPACE ADMINISTRATION

Goddard Space Flight Center

Policy Review:
What Every Webmaster Should Know

Emma Antunes
Goddard Web Manager
December 13, 2005



Introduction

- Legal Context of NASA Policy
- High Level Requirements
- Content
- Accessibility
- Presentation
- Adminisitrivia

Legal Context of NASA Policy

- Where do these rules come from?
  - Federal Law
  - OMB Memos (guidance on how to implement the law)
  - NASA policy (guidance on how to implement OMB requirements)
  - Goddard policy (mostly procedures)

WWW Regulations and Policies

Federal Legislation

- Privacy Act of 1974, as amended
- Computer Security Act of 1987
- Paperwork Reduction Act of 1995
- Clinger-Cohen Act of 1996
- Electronic Freedom of Information Act (EFOIA) Amendments of 1996
- Section 508 of the Rehabilitation Act Amendments of 1998
- Children's On-line Privacy Protection Act of 1998 (COPPA)
- Government Paperwork Elimination Act of 1998
- Section 646, Protection Of Citizens' Privacy On Federal Web Sites, Treasury And General Government Appropriations Act, 2001 (P.L. 106-554, December 21, 2000)
- E-Government Act of 2002
- Homeland Security Act of 2002
- Executive Order 12862, Setting Customer Service Standards
- Executive Order 13011, Federal Information Technology
- Executive Order 13166, Improving Access to Services for Persons With Limited English Proficiency

OMB/Dept. of State/Dept. of Commerce

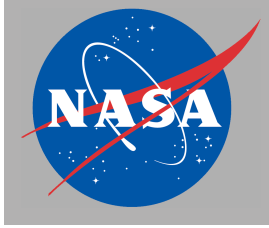
- Privacy Policies and Data Collection on Federal Web Sites (OMB "Cookie" Memo)
- Privacy Policies on Federal Web Sites, OMB, June 2 1999
- OMB Circular No. A-130, Management of Federal Information Resources.
- U.S. Export Administration Regulations (EAR)
- International Traffic in Arms Regulations (ITAR)
- Memorandum for Chief Information Officers and Federal Webmasters: Top Privacy Principles for Federal Web Sites (GSA)
- OMB Information Quality Guidelines (October 1, 2002)
- OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB Policies for Federal Agency Public Websites

NASA

- NPD 1382.17, Privacy Act - Internal NASA Direction in Furtherance of NASA Regulations
- NPD 1440.6, NASA Records Management.
- NPR 1441.1, NASA Records Retention Schedules.
- NPD 2190.1, Procedures and Guidelines for the NASA Export Control Program
- NPR 2190.1, Procedures and Guidelines for the NASA Export Control Program
- NPD 2800.1, Management of Information Technology
- NPR 2800.1, Management of Information Technology
- NPD 2810.1, Security of Information Technology
- NPR 2810.1, Security of Information Technology
- NITR 2810-3, NASA Internet Publishing Content Guidelines
- NPR 2200.2, Guidelines for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information
- NPD 2220.5, Management of NASA Scientific and Technical Information
- NASA STD 2804.I, Minimum Interoperability Software Suite
- Designated Internet Home Page Naming And Ownership (CIO Executive Notice 08-95)
- NASA Public Affairs Internet Communications Policy, Oct 95
- Policy for Retention of Internet Services Server Log Files (CIO Executive Notice 23-97, based on Schedule 2, Item 13 of the NASA Records Retention Schedule,)
- Guidance on Implementation of Information Technology (IT) Security Warning Banners (CIO memo dated October 10, 1997)
- Guidance on Implementation of NASA Website Privacy Statement (CIO memo dated June 1, 1998)
- Logo Policy (Associate Administrator for Public Affairs memo dated June 2000)
- NASA Web Site Registration and Internet Policy (Dated 11/15/01)

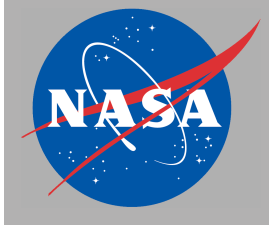
GSFC

- Authorized Use of the Internet, the World Wide Web (WWW) and Related Internet Services (Center Announcement #95-02)
- GSFC Policy and Responsibilities for the Use of the World Wide Web (WWW) Technology (Center Announcement #95-04)
- GPR 2800.1, GSFC Section 508 Web Compliance



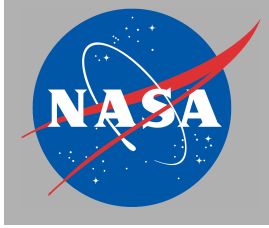
High Level Requirements

- Coding Standards
- Web Security
- Appropriate Use



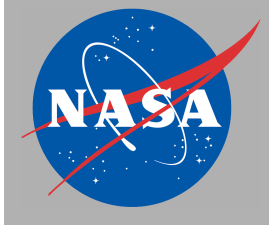
High Level: Coding Standards

- NASA STD 2804.I
  - Interface Standard
    - W3C and **industry standards**, including the following:
      - HTML 4.01, XHTML 1.0, CSS (Cascading Style Sheets), ECMAscript (JavaScript)
    - Capability to run Java 2 applets
    - SSL version 2 and 3 using 128 bit RC4 encryption and the MD5 message digest algorithm.
  - Product Standard
    - Windows: IE 6 and Mozilla Firefox 1.0.4+
    - Mac OS X: IE 5.2.3 and Mozilla Firefox 1.0.4+, and Safari 1.3+
    - Other Unix: Mozilla Firefox 1.0.4+
- What this means:
  - Code to the spec, not the browser.
  - Web sites must work in multiple browsers



High Level: Web Security

- Follow NPR 2810
- Use appropriate access restriction
- Lock down your system
- Follow good password practices
  - No group passwords
  - No passwords in plain text email
- Programmers and sysadmins for a system should communicate well and often
- Follow good application programming practices…



Top Ten Application Security Flaws
From http://www.owasp.org

1	Unvalidated Input	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.
2	Broken Access Control	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
3	Broken Authentication and Session Management	Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
4	Cross Site Scripting (XSS) Flaws	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
5	Buffer Overflows	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.
6	Injection Flaws	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.
7	Improper Error Handling	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
8	Insecure Storage	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
9	Denial of Service	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
10	Insecure Configuration Management	Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

High Level: Appropriate Use

- Must be work related
  - Same guidelines apply as everywhere else
- Remember: every Web page represents NASA
- Limited professional pages allowed
  - Work-related bio, photo, links to projects OK
  - Resume/CV not OK

Content

- Internet Content Guidelines
- Export Control/STI
- Linking Policy
- Privacy
- COPPA
- Web Surveys

Content: Internet Content Guidelines

- Now NITR 2810-3
- Governs what may and may not be published on the public Internet
- Addresses Homeland Security concerns
  - Physical location & capability information
  - Export controlled information
  - IP addresses, Network configuration, OS & version
    - Hi, I'm Apache version 1.3 for Linux! Hack me!
- What this means:
  - Don't give hackers and terrorists info they can use against us

Content: Export Control/STI

- Export-controlled material on Web sites must be restricted.
  - Use 3 levels of restrictions
    - Encrypted Channel
      - SSH, SSL, VPN, IP sec; Meets FIPS requirements
    - Controlled Delivery
      - ACL, Authorized users, restricted to US Persons (or as per agreement)
    - Encrypted Data
      - PKI, PGP; encrypted disk; behind firewalls
- Web logs for servers with ITAR/EAR data must be retained a minimum of 1 year, preferably 2
- Export Control help available at http://export.gsfc.nasa.gov/websites.htm
- Export Control review part of process to obtain Web port waiver

Content: Linking Policy

- External links
  - Must be indicated as such
  - Exit page not required
- Choice of links depends on
  - Relevancy to Web site
  - Appropriateness of content
  - Non-endorsement of content
  - Trustworthiness of site/content
    - World Book Encyclopedia vs. Wikipedia?
- Review regularly
  - Be vigilant and ensure that the content you're linking to hasn't changed significantly

Content: 3rd Party Code

- Related to linking: using 3rd party code
  - Example: Google's Urchin Service, Clicktracks, 3rd party cookies
  - Considered "web bugs"
  - You get metrics; they get surfing habits and more
- Violates NASA Privacy Policy
  - "At no time is private information you have given us, whether stored in cookies (persistent) or elsewhere, shared with third parties that have no right to that information."
- Memo likely coming early next year
- Possible waiver process likely similar to rules for persistent cookies
  - e.g. Compelling need, prominent notice, permission from the NASA administrator

Content: Privacy

- New Privacy policy to be issued this week
  - Deadline for implementation: Dec 31
    - Best effort, given the holidays
  - Two elements:
    - Text version (Banner)
    - Machine readable Privacy policy
- Banner
  - Privacy policy, IT security warning, accessibility notice and linking disclaimer are combined to become "NASA Web Privacy Policy"
  - Good news: Banner is no longer required to be local
    - Exception: in the case of cookies, privacy data, or COPPA, where additional information is required
  - New: link to banner with the text "Privacy Policy and important notices"
  - COTS not exempt from banner requirement.

Content: Privacy

- Machine Readable privacy policy (P3P)
  - Required on all public sites
  - Guidance available for simple sites, complex sites are TBD
    - Simple = no forms, cookies (of any kind), or collection of privacy data
  - Bad news: Must be local, in defined location: ex. host.gsfc.nasa.gov/w3c/
- More information at http://insidenasa.nasa.gov/ocio/information/info_privacy/

Content: COPPA

- COPPA = Children's Online Privacy Protection Act
- Governs information gathering online from or about children under the age of 13.
  - Verifiable consent from a child's parent or guardian is required before collecting, using, or disclosing personal information from a child under the age of 13.
- If COPPA applies, the web site must specify:
  - Contact information for the operators of the site
  - Information collected
  - What the information will be used for
  - Who will see it
  - How long it will be kept.
- Good example of COPPA notice at NASA kids:
  - http://kids.msfc.nasa.gov/

Content: Web Surveys

- Surveys of 10 or more members of the public must be approved by OMB
  - Falls under the Paperwork Reduction Act
  - Addressed briefly in NPR 2800
- Surveys of employees must be vetted by Labor Relations
- Not a lot of NASA guidance available that's geared to webmasters

Accessibility

- What is Section 508?
  - Access to Electronic and Information Technology for users with disabilities
  - 16 checkpoints for Web site accessibility
    - Address color, alternate text, tables and forms, multimedia
  - Good tutorial on Section 508 at
    - http://usability.gov/web_508/tutorial.html
  - Goddard Web Accessibility Coordinator:
    - Courtney Smith Courtney.L.Smith@nasa.gov 6-7946
  - More info at http://web508.gsfc.nasa.gov/

Accessibility

- New: GPR 2800.1
  - Requires that Goddard Web sites be accessible
  - Establishes:
    - Process for how sites will be tested/reviewed for accessibility
    - How accessibility will be enforced
  - Procedures for implementation of this policy are still under development

Presentation

- Logo Use
- NASA Look & Feel

Presentation: Logo Use

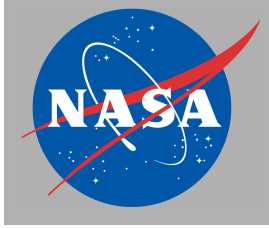
- Only the NASA meatball may be used; no other logos permitted
  - Sites hosted jointly with NASA partners excepted
- Thumbnails of project logo, center logo used for navigation included in restriction
- TISB (Code 293) is responsible for NASA Graphics Standards
  - See http://tisb.gsfc.nasa.gov/ for more info

Presentation: NASA Look & Feel

- What is this "Portal" thing?
  - NASA.gov web site, distributed hosting environment, Content Management System (CMS), and look & feel
  - Intended for Public sites
    - Popular/significant sites, major events
- NASA Look & Feel on all public sites
  - Recommendation, not requirement
  - Affinity = how much a site looks like the NASA Portal
    - While there's a range of affinity, don't mess with the way the navigation works

Presentation: NASA Look & Feel

- Resources available
  - NASA Affinity Kit
    - http://www.hq.nasa.gov/pao/portal/affinityKit
  - Portal CSS
    - http://portalcss.gsfc.nasa.gov
  - Portal Affinity Graphics Generator
    - http://portalgraphics.gsfc.nasa.gov

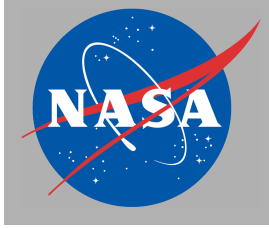


Adminisitrivia

- Responsible contacts
- Log Retention
- Metatags
- Server Configuration
- Web Port Waivers

Adminisitrivia: Responsible contacts

- Contacts required at the bottom of the front page of every Web site
  - Responsible NASA Official (RNO) name and contact information
    - Must be civil servant
    - Curator/webmaster can't also be the RNO. Should be a supervisor.
  - Webmaster name and contact information
    - May be broken down into "curator/content owner" and "technical contact"
  - Must specify a person's name, not a group
  - Email may go to a list or web form, so long as we know who the responsible party is



Adminisitrivia: Log Retention

- No server logs may be kept beyond 60 days
  - Means that you can have current log and previous month's
  - Logs beyond that must be dumped regularly
- Security exemptions permitted
  - Must be approved
- Part of NASA's records retention schedule

Adminisitrivia: Metatags

- Meta-tags must be included in the `<head>` of the front page of the Web site
  - **title**: Title of Web site
  - **description**: Short Description of Web Site
  - **orgcode**: Owning Organization Code
  - **rno**: Responsible NASA Official Name
  - **content-owner**: Content Owner name
  - **webmaster**: Technical Webmaster name (multiple webmaster tags allowed)
    - Names must be in X.500 permanent email address format

  Examples:

  - `<meta name="description" content="NASA's Constellation X-Ray Mission project office home page.">`
  - `<meta name="orgcode" content="920">`
  - `<meta name="rno" content="William.J.Clinton.1">`
  - `<meta name="content-owner" content="Emma.K.Antunes.1">`

Adminisitrivia: Server Configuration

- Every server must have a page at the root level that responds to web requests, even if the site home page is not located at the root level.
  - This page must also include banners and information about owning organization
- No directory listings at the root level
- The default home page at the root level may not be a user's personal page, even if it's work-related.
  - This implies that the user is the reason for the site's existence; it has the appearance of self-promotion or inappropriate use
  - Use http://server.gsfc.nasa.gov/~username or http://server.gsfc.nasa.gov/username/

Adminisitrivia: Web Port Waivers

- Streamlined Waiver process for Web ports (80, 8080, 443)
- Ensures basic review of public Web sites for compliance with:
  - STI/Export Control
  - Required info on front page
  - Section 508
  - Logo use
  - In the Web Registry
- Waivers good for one year
- See http://webmaster.gsfc.nasa.gov/ for more info, or email web-port-waiver@majordomo

Conclusion

- More detailed information is available from http://webmaster.gsfc.nasa.gov/
- Questions?
- Contact info:

Emma Kolstad Antunes
Goddard Web Manager
emma.k.antunes@nasa.gov
286-1377